DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

IN REPLY REFER TO
NAVSEAINST 2200.1A
SEA 00I/198
29 Apr 2019

NAVSEA INSTRUCTION 2200.1A

From: Commander, Naval Sea Systems Command

Subj: PORTABLE ELECTRONIC DEVICES POLICY

Ref: See Enclosure (1)

Encl: (1) Reference List
(2) Portable Electronic Devices Prohibited Capabilities Matrix
(3) Government Property Pass Form Instructions

1. Purpose

a. This instruction assigns responsibilities for the Naval Sea Systems Command (NAVSEA) Portable Electronic Device (PED) policy and sets minimum security requirements for PED use.

b. Exclusions. This instruction does not:

(1) Alter or supersede the existing authorities and policies regarding the protection of sensitive compartmented information (SCI), as directed in reference (a) and other laws and regulations.

(2) Alter or supersede the existing authorities and policies regarding the protection of special access programs (SAP).

(3) Apply to properly credentialed law enforcement, including Naval Security Force, or Inspector General personnel in performance of their official duties.

(4) Apply to equipment exempted by higher guidance; specifically, per reference (b): receive-only pagers, Global Positioning System receivers, hearing aids, pacemakers, other implanted medical devices, or personal life support systems all of which are allowed in all NAVSEA spaces.

(5) Alter the responsibilities of the Deputy Administrator for Naval Reactors set forth in reference (c) and the Under Secretary for Nuclear Security, Department of Energy, set forth in reference (d).

2. Cancellation. NAVSEAINST 2200.1 of 2 February 2015 and NAVSEA Memo of 14 April 2016.

3. Applicability. This instruction applies to the NAVSEA enterprise, affiliated Program Executive Offices, per reference (e), and field activities.

4. Background. Introduction of PED poses a risk to the protection of classified information and controlled unclassified information (CUI), including Naval Nuclear Propulsion Information (NNPI) as defined in reference (f). Various capabilities of PED could permit direct exfiltration of information (e.g., cameras, microphones), indirect exfiltration of information via compromising electromagnetic emanations, and introduction of malicious capabilities to Navy information systems. Because of the fast pace of PED evolution, it is impractical to develop policy regarding PED based on device type or form factor; instead, it is imperative that policy governing these devices is focused on a device's capabilities.

5. Definition

a. PED is defined in reference (g) as a portable electronic device having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of PED include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistants, audio devices, watches with input capability, reminder recorders, and mobile devices.

b. Mobile devices are a type of PED further defined in reference (g) as a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices also include voice communication capabilities, onboard sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.

c. For the purposes of this instruction, PED and mobile device are synonymous. This instruction applies to all devices broadly meeting the PED definition and includes government owned, contractor owned, and personally owned PED within NAVSEA spaces enterprise wide.

d. Near Field Communication (NFC) is defined as a short-range wireless communication system employing radio waves to enable a mobile device to interact with another device or card reader when within 10 cm (4 in) of each other.

e. Computer cellular wireless service (including air or data cards) is to be treated the same as phone based cellular wireless service with regard to spaces where its use is allowed or prohibited.

f. Personal Wearable Fitness Devices (PWFD) are a type of PED with limited functionality for fitness tracking. Permitted PWFD, as defined in reference (h), typically include Bluetooth,

receive only Global Positioning System, accelerometer, altimeter, gyroscope, heart activity, vibration feature, and NFC capabilities.

6. Responsibilities

a. Commanders, commanding officers, and officers in charge (hereinafter "local commanders") must establish a risk based local PED policy to ensure PED use is consistent with protecting classified information and CUI from unauthorized disclosure per reference (i). Local commanders must also ensure that all personnel must acknowledge and comply with local PED policy. The local PED policy must include:

(1) Identification of spaces where PED are prohibited and prohibited PED capabilities, this may include spaces where the use of personally owned PED would represent a worker safety issue, workplace productivity issue or an unacceptable risk due to heightened operations security concerns;

(2) The local command approval process for exceptions to the local PED policy;

(3) Individual responsibility to use PED per policy and to prevent imaging, recording, or exporting of classified information or CUI; and

(4) The consequences for violation of the local command policy, including PED seizure, administrative, and/or disciplinary actions that may negatively impact continued access to classified information or CUI.

b. Command Information Systems Security Managers (ISSM) are responsible for:

(1) Coordinating use of Wi-Fi and Wi-Fi hotspots;

(2) Reviewing PED for purposes of reasonable accommodation, as described in paragraph 7l of this instruction; and

(3) Advising the local commander on exceptions to this policy.

c. Command Security Managers (CSM) are responsible for:

(1) Reviewing PED for purposes of reasonable accommodation, as described in paragraph 7l of this instruction;

(2) Advising the local commander on exceptions to this policy;

(3) Implementing appropriate measures to ensure compliance with this policy per reference (i);

(4) Reporting, recording, investigating, and referring violations of this policy, as appropriate, per reference (i).

d. Supervisors are responsible for:

(1) Enforcing policy to avoid violations;

(2) Initiating appropriate administrative and disciplinary action in the event of a violation.

(3) Notifying the CSM of violations to the PED policy.

7. Action. PED are prohibited within spaces authorized for processing classified information, or within spaces where any classified discussion is taking place, except as otherwise authorized. PED are permitted in other areas, subject to the restrictions of the local PED policy and subject to the usage restrictions as follows:

a. PED may not be connected to Government information systems unless explicitly allowed in the information system's authorization to operate (ATO) documentation per reference (j). Government PED may not be physically connected to personally owned computer systems. Backing up Government PED on personal computer systems is prohibited.

b. Personally owned peripherals (e.g., keyboards, mouses, headphones) may not be connected to government PED, with the exception of analog audio (headphones/speakers) or monitors connected via one-way (PED to monitor) analog or digital connections.

c. Personally owned wireless peripherals (i.e., Bluetooth headphones, speakers, etc.) are authorized for use with personally owned PED. Contractor owned wireless peripherals are authorized for use with contractor owned PED.

d. Navy enterprise managed PED (e.g., Navy Marine Corps Intranet (NMCI)) are permitted to be brought into NAVSEA spaces per the stipulations in paragraph 7f for classified spaces and paragraph 7g for unclassified naval nuclear propulsion spaces, and do not require unique local command approval.

e. PWFDs may be used per reference (h); "Cyber Hygiene Authorization to Use Personal Wearable Fitness Devices in Navy Spaces".

f. PED in Classified Spaces. Limited use of PED in classified processing spaces, including but not limited to open storage areas, controlled access areas, nuclear work areas, and nuclear propulsion plant spaces onboard ships:

(1) Consistent with reference (k), in spaces where classified SECRET and CONFIDENTIAL collateral information is processed, transmitted, stored, or discussed, PED with limited capabilities are permitted:

(a) If commercially obtained in the U.S. or through U.S. military exchange.

(b) If assigned a Federal Communications Commission (FCC) identifier denoting compliance with the limits for a Class B digital device (e.g., consumer grade electronics including laptops, tablets, and cellphones, etc.) designated by the FCC, pursuant to Part 15 of the FCC Rules, per reference (l). Class B devices are designated by the FCC as suitable for use by the general public in residential and commercial, business and industrial environments.

(c) If they contain only government approved software and/or vendor-supplied software, and receive only updates that do not add any features or capabilities prohibited in paragraph 7g(2).

(d) If they have any or all of the following allowed capabilities: Bluetooth, receive only Global Positioning System, accelerometer, altimeter, gyroscope, heart monitor, vibration, and/or NFC capabilities, but none of the prohibited capabilities in paragraph 7g(2) of this instruction.

(e) Spaces that process information that is not categorized as collateral information (e.g., information categorized as "Restricted Data" under the Atomic Energy Act) should follow rules established by the applicable original classification authority.

(2) The following capabilities are prohibited on PED in classified spaces:

(a) Cellular and Wi-Fi transceivers. NMCI unclassified laptops with embedded Wi-Fi are authorized for use in classified spaces per reference (m) which requires laptops be physically connected to the unclassified network before powering on or have Wi-Fi disabled prior to entry into the space.

(b) Photographic, video capture, recording, and transmission, microphone, and/or audio capture, recording, and transmission capabilities.

(c) Installed removable media.

(d) Capability to perform radio frequency transmission at greater than 100 milliwatts (mW) Equivalent Isotropically Radiated Power as, where feasible, determined using FCC data.

(3) If a space (e.g., individual office or conference room) is intermittently used for processing or discussing classified information, positive action must be taken to remove PED with prohibited capabilities from the space before classified information is processed or

discussed. If classified information must be transported through areas where PED with prohibited capabilities are present, the classified information must be protected to ensure that the presence of PED does not inappropriately disclose the information.

(4) Per reference (n), the use of government owned PED is permitted in Naval Nuclear Propulsion Program Emergency Control Centers during drills and emergencies, regardless of their radio frequency capabilities.

(5) Use of PED in spaces processing information at a level higher than SECRET collateral is not permitted unless explicitly allowed in the information system's ATO documentation per reference (j).

g. PED in U-NNPI Spaces. Consistent with reference (o) in spaces where U-NNPI is processed, transmitted, stored, or discussed (e.g., Security Islands, Controlled Nuclear Information Areas), PED are permitted as follows:

(1) Where U-NNPI information is processed or stored in its material form or physical manifestation (e.g., industrial processes, material), personally owned PED with photographic, video capture, and recording, and transmission, microphone, and/or audio capture, recording, and transmission capabilities are prohibited. Government and contractor owned PED are permitted in these areas provided they have their photographic and video capabilities (logically or physically) disabled, and they have been marked to identify that the capability is disabled as specified in paragraph 7g(3) of this instruction.

(2) The possession and appropriate limited use of PED capable of recording, transmitting or exporting photographic images and audible information in office spaces containing and/or processing U-NNPI, wherein only paper documents and screens (e.g., computer screens, monitors) displaying NNPI are present, represents a sufficiently low risk and is permitted.

(3) Organizations that logically disable photographic and video capabilities using mobile device management solutions must develop and maintain programs to mark PED that have been logically disabled. These programs must provide a serialized, tamper evident marking to annotate the photographic and video capabilities are disabled; the label must identify the organization that applied the label, and it must be visible on PED even when contained within a case. All NAVSEA organizations should honor the markings of other NAVSEA organizations and contractors.

(4) In locations where the Controlled Industrial Area (CIA) as defined by reference (o) serves as both an access control boundary and an information security boundary, then PED capable of recording, transmitting or exporting photographic images and audible information are prohibited within the CIA unless their photographic and video capabilities have been disabled. Consistent with reference (o), members of ship's force who are assigned living quarters aboard ships or living barges within the CIA may transit directly to and from the CIA entrance nearest

the ship or barge while carrying PED with prohibited capabilities. This privilege is not authorized for personnel who have living quarters outside the CIA, nor for the duty section aboard the ship or barge. Devices that are being transported must be powered down and not visible to passers-by.

h. Wi-Fi and Wi-Fi Hotspots. Use of wireless hotspots must be coordinated with Command ISSM to ensure usage does not interfere with official-use wireless capabilities or the effectiveness of wireless intrusion detection systems. The use of Wi-Fi hotspots is authorized as follows:

(1) Wi-Fi hotspots are not authorized in spaces in which classified material is being handled, processed, or discussed unless explicitly allowed by the information system's ATO documentation per reference (j). A Tempest evaluation conducted by a Certified Tempest Technical Authority must be done prior to installing Wi-Fi hotspots in a building that contains classified spaces.

(2) Wi-Fi hotspots are not authorized in areas directly adjacent to SCI spaces or SAP spaces without the prior authorization of the cognizant special security officer or SAP control officer.

(3) Navy enterprise provided wireless solutions, to include Wi-Fi hotspots and Wi-Fi hotspot capability on Navy enterprise provided PED (e.g., Navy issued Government cellphones and laptops), are authorized for use within NAVSEA per its Navy approved configuration, but use must be coordinated with the Command ISSM to de-conflict with wireless intrusion detection systems.

(4) Contractor owned and Government owned (but not provided as an approved Navy enterprise solution) Wi-Fi hotspots may be used within NAVSEA spaces, but must be coordinated with the Command ISSM.

(5) Personally owned Wi-Fi hotspots are not authorized. The Wi-Fi hotspot function on personally owned PED must be turned off while in NAVSEA spaces.

(6) Dual homing (connecting to both wireless and wired networks simultaneously) is prohibited unless explicitly allowed by the information system's ATO documentation per reference (j).

i. Classified PED. NAVSEA personnel may use approved classified PED per the requirements defined in reference (p). Requests for Department of Defense (DoD) Mobility Classified Capability PED must be approved by the Command Information Office (SEA 00I) Enterprise Authorized Approving Official for the Defense Information Systems Agency (DISA) service requests.

j. In areas where PED is authorized, the use of recording or imaging capabilities built into PED are subject to the restrictions in reference (o).

k. Reasonable Accommodation. Government issued PED, including recording devices, may be approved for use through the reasonable accommodation (RA) process on a case-by-case basis for individuals with disabilities. The Command ISSM and CSM must review the PED as part of the RA interactive process to ensure the device does not introduce an unacceptable risk. Recording devices approved through the RA process must be issued a permit per reference (o), tracked for accountability, and disposed of per reference (q).

l. Property Passes. All NAVSEA Commands are required to issue property pass guidance for all Government-owned equipment exiting its spaces per reference (r). When issuing property passes for PED, the General Services Administration (GSA) is the only authorized property pass form per reference (s) that will be accepted within the NAVSEA enterprise.

(1) Property passes for PED will be issued for no more than a twelve-month period.

(2) Enclosure (3) provides guidance on how property passes using reference (s) will be completed for PED.

(3) Reference (s) will not be used when other forms are directed for use as appropriate documentation, for example, forms such as the DD Form 1149 (Requisition and Invoice/Shipping Document) or DD Form 1348-1 (Issue Release/Receipt Document).

m. Exceptions. The integration and capabilities of PEDs have the potential to bring significant efficiencies to the workforce. As such, it is imperative that commands evaluate the business justification and security risks on a case-by-case basis when there are clear operational benefits of using PEDs that are prohibited based on this high-level policy. Local commanders, with consultation from their ISSM and CSM, are authorized to allow Government and contractor-owned PEDs with prohibited capabilities into classified and unclassified naval nuclear propulsion information processing spaces to support operational requirements if the prohibited capability can be disabled in a verifiable and technically sound manner (e.g., tamper proof tape over a camera, spot check process with a signal detector for wireless disablement, etc.). Local commanders must adhere to the requirements of reference (b), including gaining approval from the appropriate Authorizing Official and Certified Tempest Technical Authority prior to authorizing exceptions for wireless capabilities prohibited by this instruction. In all cases, exceptions must be documented in writing, approved by the local commander, and include discussion of the business need, pertinent risks, and how the risks are mitigated. Additionally, if categories of proscribed information (e.g., Restricted Data, Formerly Restricted Data, COMSEC information) are processed in the subject spaces, the waivers from this policy must also receive concurrence from the respective data owner.

n. Disciplinary Action. Discovery of PED in prohibited areas, or discovery of prohibited materials (including Government information or digital photographs that have not been authorized for public release per reference (i)) on personally owned PED, may result in the immediate confiscation of the device by the CSM and referral to the appropriate authorities for investigation and, if warranted, personnel action or prosecution.

(1) Civilian employees failing to comply with the requirements of this instruction are subject to disciplinary action per guidance provided in reference (t).

(2) Military members failing to comply with the requirements of this instruction are subject to disciplinary action per the Uniform Code of Military Justice.

(3) Contractors found to be in violation of this policy will have the violation reported to their contracting officer's representative and may be subject to criminal charges.

(4) Visitors found to be in violation of this policy will be reported to the CSM and may be subject to criminal charges.

8. Records Management

a. Records created as a result of this instruction regardless of format or media, must be maintained and dispositioned for the standard subject identification codes (SSIC) 1000 through 13000 series per the records disposition schedules located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction [notice, change transmittal] or the records disposition schedules, please contact your local records manager.

9. Review and Effective Date. Per OPNAVINST 5215.17A, SEA 00I will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, Secretary of the Navy (SECNAV), and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

10. Forms. General Services Administration (GSA) Optional Form 7 Property Pass is available from the GSA Forms Library at: https://www.gsa.gov/forms-library/property-pass.

T. J. MOORE

Releasability and distribution:
This instruction is not cleared for public release and is available electronically only, via the NAVSEA Intranet Website located at https://navsea.portal.navy.mil

REFERENCE LIST

(a) E.O. 12333, United States United States Intelligence Activities, as amended
(b) DoD Directive 8100.02 of 14 April 2004
(c) 50 U.S.C. §2406, Deputy Administrator for Naval Reactors
(d) 42 U.S.C. §7158, Naval Reactors and Military Application Programs, as amended
(e) "Operating Agreement Between the Commander, Naval Sea Systems Command, and NAVSEA's Affiliated Program Executive Officers", of April 1997
(f) OPNAVINST N9210.3
(g) Committee on National Security Systems Instruction No. 4009 of 6 Apr 2015
(h) NAVADMIN 216/15, Cyber Hygiene Authorization to use Personal Wearable Fitness Devices
(i) SECNAV M-5510.36 of 1 June 2006
(j) DoD Instruction 8510.01 of 12 March 2014
(k) ALNAV 019/16, Acceptable Use of Authorized Personal Portable Electronic Devices
(l) FCC Office of Engineering and Technology Bulletin 65
(m) NAVADMIN 290/15, Use of Unclassified Navy and Marine Corps Intranet Laptops with Embedded Wireless
(n) FLTCYBERCOM Ser NAO/1843 of 6 Nov 2015, Waiver Request for use of Cellular Phones in Naval Nuclear Propulsion Program Emergency Control Centers
(o) NAVSEAINST 5510.2D
(p) Navy Security Note 08-15, Guidance on the Proper Use of DOD Mobility Classified Capability-Secret (DMCC-S) Device and Other Authorized Classified PED
(q) DON CIO Message DTG 281759Z AUG12, Processing of Electronic Storage Media for Disposal
(r) NAVSEAINST 7320.1A
(s) SECNAVINST 12752.1A

PORTABLE ELECTRONIC DEVICES PROHIBITED CAPABILITIES MATRIX

Green: Allowed unless otherwise restricted by local Command policy
Yellow: Government and Contractor owned PED only
Red: Prohibited

	Unclassified Spaces	U-NNPI Office Spaces	U-NNPI Material/ Physical Spaces	Collateral SECRET/ CONFIDENTIAL Spaces	Collateral TOP SECRET Spaces	SCI/SAP Spaces
Bluetooth, receive only GPS, accelerometer, altimeter, gyroscope, heart monitor, vibration, and/or NFC						
Non-government approved 3rd Party Apps						
Cellular and Wi-Fi Transceivers			Government/ Contractor Owned Only			
Photographic, Video, Audio Capture and Transmission						
Installed Removable Media						
RF transmission > 100 mW						

U-NNPI Material/Physical Spaces: Where U-NNPI information is processed or stored in its material form or physical manifestation (e.g., industrial processes, material).

U-NNPI Office Spaces: Office spaces containing and/or processing U-NNPI, wherein only paper documents and screens (e.g., computer screens, monitors) displaying NNPI are present.

GOVERNMENT PROPERTY PASS FORM INSTRUCTIONS

General Services Administration Optional Form (OF 7) is the only authorized property pass form that will be accepted within the NAVSEA enterprise. The fields of the OF 7 will be filled out as follows:

Block 1: Date issue.

Block 2: Name. Individual authorized to have equipment in their possession. Name cannot be assigned to a Group name.

Block 3: Building. Use the text "All NAVSEA Buildings"

Block 4: Description of property being removed. This block must include brand and type (i.e., HP Laptop, Dell Laptop), serial number and Asset ID (for NMCI devices with an Asset ID).

Block 5: Property belongs to. Document owning Directorate, PEO or NAVSEA Activity down to the Shop or Code where applicable.

Block 6: Department or Agency. Use text "NAVSEASYSCOM"

Block 7: Name and signature of person authorizing removal of property:

- For IT Equipment at NAVSEA HQ: department/directorate/PEO ACIO

- For NAVSEA Activities: Follow local policy for who is authorized to issue property passes

- Digital signatures are authorized

Block 8: Title of individual in Block 7.

Block 9: Pass Good Until. Not to exceed 12 months from date issued.